Screencast: 19-firewalls.webm or 19-firewalls.mp4

REFERENCES

LaUSAH - Section 27.8 Firewalls
RHEL7 Security Guide, Chapter 5, Using Firewalls

SERVICES AND PORTS

Looking at the `/etc/services` file you will see a long list of the most well known services. Ports 1024 and lower are considered to be "privileged" ports and traditionally require root privileges to start up software that bind to them.

User's programs can usually bind to any ports 1025 and higher.

Just because a daemon / service is typically associated with a particular port or range of ports does not mean that it has to use those ports. Most applications can be configured to use whatever port(s) desired. Therefore do not assume that if a particular port is in use that a particular app is using it. Remember you are free to name binaries anything you want and sometimes unauthorized users try to be tricky.

IPTABLES OVERVIEW

- Filtering is performed by the network stack within the kernel
- Asserts policies at OSI Reference Model layers 2, 3 and 4
- Only packet headers are inspected

FIREWALLD OVERVIEW

- Red Hat introduced a new firewall system with the release of RHEL7, named firewalld
- There is a firewalld GUI named `firewall-config` and a CLI program named `firewall-cmd`.
- firewalld supports multiple zones

USING FIREWALLD

Check to see if firewalld is running:

```
systemctl status firewalld
```

firewalld stores its rules in:

```
/etc/firewalld/zones/public.xml
```

```
firewall-cmd --state
firewall-cmd --get-active-zones
firewall-cmd --list-all

firewall-cmd --add-service=http
firewall-cmd --add-service=http --permanent
firewall-cmd --remove-service=http
firewall-cmd --remove-service=http --permanent

firewall-cmd --add-port=30000/tcp --permanent
firewall-cmd --add-port=30000-30010/tcp --permanent
firewall-cmd --remove-port=30000/tcp --permanent
firewall-cmd --remove-port=30000-30010/tcp --permanent
```

```
firewall-cmd --reload
firewall-cmd --complete-reload
firewall-cmd --query-panic
firewall-cmd --panic-on
firewall-cmd --panic-off
```

FIREWALLD SERVICE FILES

```
firewall-cmd --get-services
   /usr/lib/firewalld/services/{service-name}.xml
firewall-cmd --info-service={service-name}
```

Drop-in Files:

```
   /etc/firewalld/services/
```

FIREWALLD ADVANCED FEATURES

Direct Interface
Rich Rules
Lockdown
IP Sets